

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-366437

(43)Date of publication of application : 20.12.2002

(51)Int.Cl. G06F 12/14
H04L 9/10

(21)Application number : 2001-168974 (71)Applicant : SHARP CORP

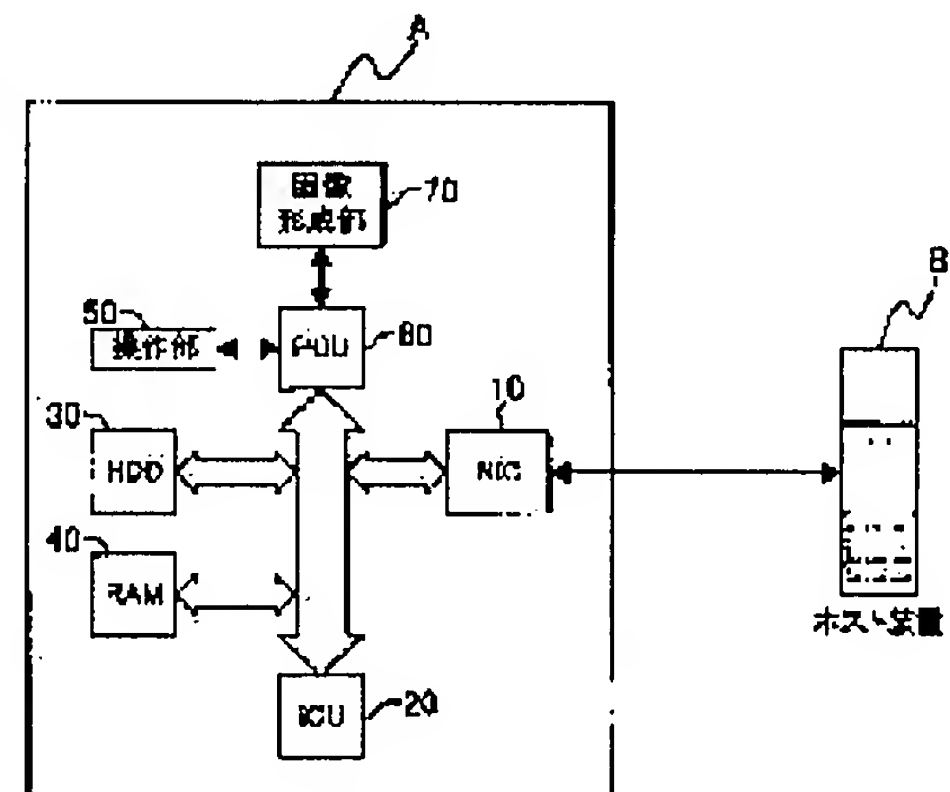
(22)Date of filing : 05.06.2001 (72)Inventor : TORII MIKIO
NAKAI YASUHIRO

(54) ENCRYPTION PROCESSOR AND ENCRYPTION PROCESSING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an encryption processor and encryption processing system capable of efficiently storing and outputting data to a storage device by encrypting only received data whose encryption is necessary.

SOLUTION: An NIC 10 judges whether or not data received from a host device B should be encrypted, and when it is judged that the encryption of the data is necessary from the judged result, the data are encrypted.



LEGAL STATUS

[Date of request for examination] 17.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

THIS PAGE BLANK (USPTO)

[Date of final disposal for application]

[Patent number] 3781640

[Date of registration] 17.03.2006

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-366437
(P2002-366437A)

(43) 公開日 平成14年12月20日 (2002. 12. 20)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 Z 5 J 1 0 4

審査請求 未請求 請求項の数11 O L (全 8 頁)

(21) 出願番号 特願2001-168974(P2001-168974)

(22) 出願日 平成13年6月5日(2001.6.5)

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 島居 幹夫

大阪府大阪市阿倍野区長池町22番22号シャープ株式会社内

(72) 発明者 中井 康博

大阪府大阪市阿倍野区長池町22番22号シャープ株式会社内

(74) 代理人 100084135

弁理士 本庄 武男

Fターム(参考) 5B017 AA07 BA07

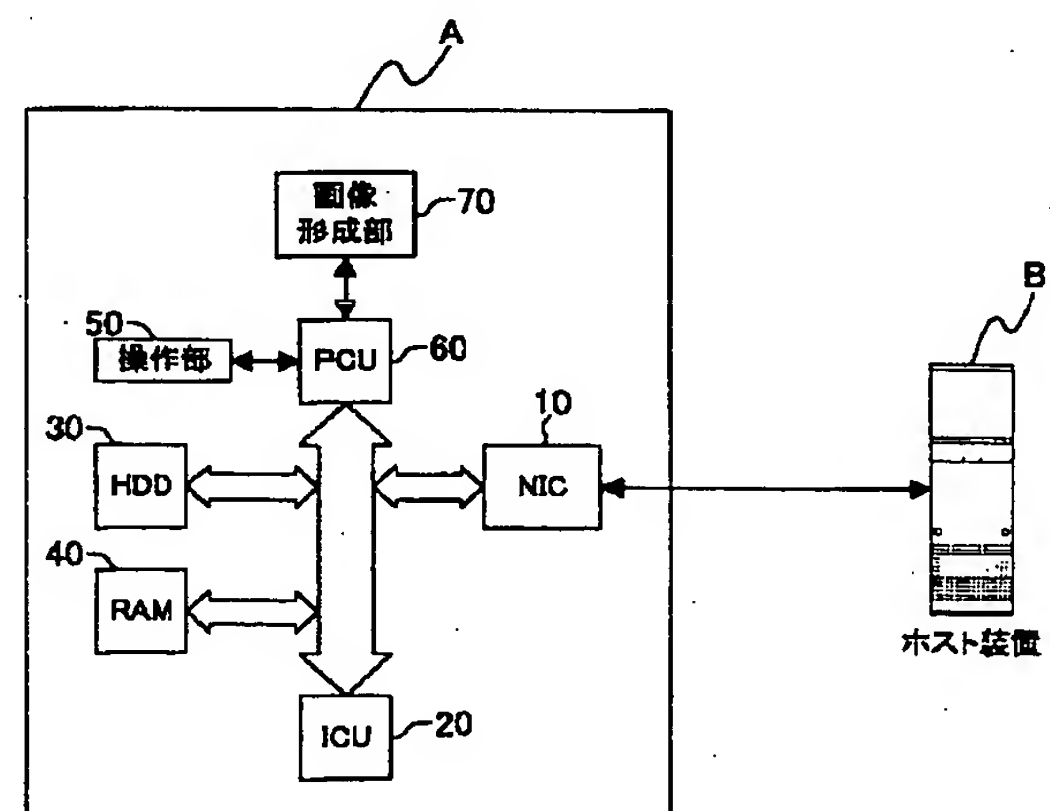
5J104 AA18 AA33

(54) 【発明の名称】 暗号化処理装置、暗号化処理システム

(57) 【要約】

【課題】 外部機器より送出されたデータを記憶装置に一旦記憶して出力するようなシステムでは、上記記憶期間中のデータの安全性を保つために、受信したデータを全て暗号化する技術が従来よりある。しかし、受信したデータの全てを暗号化すると暗号化処理の負荷が大きくなり、システム上における処理の時間の長大化の原因となって効率が悪い。

【解決手段】 NIC 10は、ホスト装置Bより受信したデータに対して暗号化が必要か否かを判断し、該判断によって上記データの暗号化が必要と判断された場合に、上記データを暗号化する。



【特許請求の範囲】

【請求項1】 受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置において、上記データに対して暗号化が必要か否かを判断するための要否判断手段を具備し、上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化することを特徴とする暗号化処理装置。

【請求項2】 前記要否判断手段は、前記記憶装置の記憶形式を判別するための記憶形式判別手段の判別結果に基いて、上記データに対して暗号化が必要か否かを判断してなる請求項1記載の暗号化処理装置。

【請求項3】 前記記憶形式判別手段によって、前記記憶装置は単体で存在する状況においても記憶している前記データを前記受信の際の状態で保存すると判別された場合に、更に前記要否判断手段は前記データに対して暗号化が必要と判断してなる請求項2記載の暗号化処理装置。

【請求項4】 前記要否判断手段は、前記データの形態又は具備する項目に基いて、前記データに対して暗号化が必要か否かを判断してなる請求項1記載の暗号化処理装置。

【請求項5】 前記データの形態が既に暗号化されている場合に、前記要否判断手段は前記データに対して暗号化が不必要と判断してなる請求項4記載の暗号化処理装置。

【請求項6】 前記データの具備する項目が前記データの重要度に関する指標である場合に、前記要否判断手段は前記データに対して暗号化が必要と判断してなる請求項4記載の暗号化処理装置。

【請求項7】 前記指標が、フラグ、親展指示等である請求項6記載の暗号化処理装置。

【請求項8】 前記データの具備する項目が予め定められた条件である場合に、前記要否判断手段は前記データに対して暗号化が必要と判断してなる請求項4記載の暗号化処理装置。

【請求項9】 前記記憶装置に暗号化して記憶されている前記データを復元するための復元化手段を具備し、該復元化手段によって前記データが復元された後に前記データが出力されてなる請求項1から請求項8のいずれかに記載の暗号化処理装置。

【請求項10】 請求項1から請求項9のいずれかに記載の暗号化処理装置の用途として、前記データの受信側の機器に採用されてなる暗号化処理装置。

【請求項11】 データの作成などのサービスを提供するホスト装置と、該ホスト装置より受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置とを具備した暗号化処理システムにおいて、上記ホスト装置は、データを上記暗号化処理装置に送信する際に、該データに対して暗号化に関する条件を付加する条件付加手段を具備し、上記暗号化処理装置

は、上記条件の有無に基いて、上記データに対して暗号化が必要か否かを判断するための要否判断手段を具備し、上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化処理装置側で暗号化することを特徴とする暗号化処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置、暗号化処理システムに関するものである。

【0002】

【従来の技術】近年、サーバ等のホスト装置より送出されたデータをメモリ、ハードディスクドライブ（以下、「HDD」と称する。）等の記憶装置に一旦記憶した後に、該記憶装置より上記データを出力するようなシステムがある。このようなシステムの代表例としては、例えば印刷システムなどある。この印刷システムは、例えば、多数のユーザによってプリンタが共有されている場合に、プリンタ側に上記記憶装置を設けることによって、多数のユーザから上記プリンタに対してデータが同時に送出されたとしても、上記記憶装置で該データを一旦記憶するので、該記憶したデータをプリンタ本体に順次出力して印刷することを可能にするシステムである。しかし、上記システムにおいて、記憶装置よりデータを出力した後に該記憶装置にデータが残存したままであると、再び該記憶装置より上記データを出力することが可能となるので、従来より、データの出力後は記憶したデータを記憶装置より消去することが一般に行われている。これは、例えば、上記データが機密性の高いデータである場合等においては有効な処理である。

【0003】

【発明が解決しようとする課題】しかし、上述の技術の場合でも、ホスト装置より送出されたデータを一旦記憶装置に記憶してから該データを出力するまでの期間中は、該データは少なくとも上記記憶装置上に存在しており、該期間中に上記データが第三者によって読み出される、或いは、該期間中に上記データが記憶装置ごと盗まれる等の可能性があり、上記データの安全性を確実に確保できているとは言い難い。そこで、特開平4-3660号公報には、ファクシミリの記憶装置で受信したデータを暗号化して記憶し、該データを扱えるユーザが上記記憶装置にデータ復元用のICカードを挿入することによって上記データを復元化して出力する技術について開示されている。しかし、上述の技術では、上記記憶装置で受信した全てのデータを暗号化するものであるため、記憶装置における処理の負担が大きくなり上記暗号化に時間が掛かることや、暗号化の必要のないものまで暗号化される不都合がある。また更に、上記データの復元化の際に上記ICカードを挿入する煩わしさがある。そこ

で、本発明は上記事情に鑑みてなされたものであり、その目的とするところは、暗号化が必要と認められる受信データのみを暗号化することによって、効率良く記憶装置に上記データを記憶して出力することを可能にする暗号化処理装置、暗号化処理システムを提供することである。

【0004】

【課題を解決するための手段】本発明は、受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置において、上記データに対して暗号化が必要か否かを判断するための要否判断手段を具備し、上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化することを特徴とする暗号化処理装置として構成されている。本発明がこのような構成されているので、受信したデータの中で暗号化が必要と認められるデータのみを暗号化することによって、従来に比べて効率良く記憶装置に上記データを記憶して出力することが可能となる。また、暗号化が不要なデータについては暗号化されないので、処理の迅速性が維持される。

【0005】本発明において、前記要否判断手段は、前記記憶装置の記憶形式を判別するための記憶形式判別手段の判別結果に基づいて、上記データに対して暗号化が必要か否かを判断するように構成されても良い。このように構成されることで、第三者によって前記記憶装置が盗難にあった場合のデータの読み出しの可能性が判別できるので、例えば、前記記憶装置のデータの保存性が低ければ盗難時にデータが消滅するので、データに対して暗号化する必要がなくなり、更に不要な暗号化を防止できる。また、前記記憶形式判別手段によって、前記記憶装置は単体で存在する状況においても記憶している前記データを前記受信の際の状態で保存すると判別された場合に、更に前記要否判断手段は前記データに対して暗号化が必要と判断しても良い。この場合も、上述同様に、前記記憶装置単体が盗難に遭ったとしても前記データの内容が第三者によって解読される可能性が無く、前記データが機密性の高いデータである場合に非常に有効である。

【0006】また、前記要否判断手段は、前記データの形態又は具備する項目に基づいて、前記データに対して暗号化が必要か否かを判断するよう構成されることが望ましい。このように前記要否判断手段が判断することによって、暗号化が必要と認められる受信データのみを選択的に暗号化することが可能となり、従来の技術に比べて効率的に前記データの暗号化を実施することが可能となる。更に、前記データの形態が既に暗号化されている場合に、前記要否判断手段は前記データに対して暗号化が不必要と判断、又は、前記データの具備する項目が前記データの重要度に関する指標（フラグ、親展指示）である場合に、前記要否判断手段は前記データに対して暗号

化が必要と判断、又は、前記データの具備する項目が予め定められた条件である場合に、前記要否判断手段は前記データに対して暗号化が必要と判断するように構成しても良い。このように構成することで、上述同様に、前記要否判断手段によって、暗号化が必要と認められる受信データのみを効率良く選択的に暗号化することが可能となる。

【0007】前記記憶装置に暗号化して記憶されている前記データを復元するための復元化手段を具備し、該復元化手段によって前記データが復元された後に前記データが出力されるように構成することが望ましい。このように本発明に復元化手段が設けられることによって、暗号化が必要と認められて暗号化された前記データを自動的に復元化して出力することが可能となる。

【0008】また、上述の暗号化処理装置の用途として前記データの受信側の機器に採用されても良く、例えば、本発明の暗号化処理装置をホスト装置とプリンタとで構成される印刷システムに採用することで、暗号化を施すべき文書のみを効率良く印刷出力することが可能となる。

【0009】また本発明をシステムとして捉えると、データの作成などのサービスを提供するホスト装置と、該ホスト装置より受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置とを具備した暗号化処理システムにおいて、上記ホスト装置は、データを上記暗号化処理装置に送信する際に、該データに対して暗号化に関する条件を付加する条件付加手段を具備し、上記暗号化処理装置は、上記条件の有無に基づいて、上記データに対して暗号化が必要か否かを判断するための要否判断手段を具備し、上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化処理装置側で暗号化することを特徴とする暗号化処理システムとして構成されている。本発明がこのような構成されているので、暗号化処理装置の要否判断手段は、上記ホスト装置側で付加された暗号化に関する条件がデータに付加されているか否かを容易に判断できるので、受信したデータの中で暗号化が必要と認められるデータのみを暗号化することが可能となる。

【0010】

【発明の実施の形態】以下添付図面を参照しながら、本発明の実施の形態及び実施例について説明し、本発明の理解に供する。尚、以下の実施の形態及び実施例は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。ここに、図1は本発明の実施の形態に係る暗号化処理装置を採用するプリンタAの概略構成図、図2は本発明の実施の形態に係る暗号化処理装置を採用するプリンタAが行う一連の処理手順を示すフローチャート、図3は図2のステップS20のサブルーチンの一連の処理手順を示すフローチャート、図4は図2のステップS50のサブルーチンの一連の処理

手順を示すフローチャート、図5は図2のステップS50のサブルーチンの別例の一連の処理手順を示すフローチャート、図6はプリンタAが行う復元処理を示すフローチャート、図7はホスト装置Bが行う条件付加の処理を示すフローチャートである。

【0011】先ず図1を用いて、本発明の実施の形態に係る暗号化処理装置を採用する機器の一例としてプリンタAの概略構成について説明する。もちろん、本発明の暗号化処理装置は、上記プリンタAのみに限定されて採用されるものではなく、本発明の暗号化処理装置を採用することで同様の効果が得られるものであれば如何なるものに採用しても良い。

【0012】プリンタAは、要否判断機能、記憶形式判別機能、復元化機能を具備すると共に外部機器（ホスト装置B）より送出される暗号化の必要なデータを暗号化するネットワークカード10（以下、「NIC10」と称する。）と、NIC10で受信したデータ等に画像処理などの各種処理を施すイメージコントローラユニット20（以下、「ICU20」と称する。）と、NIC10で受信したデータの記憶やプリンタAの動作プログラムの展開等がなされるHDD30（記憶不揮発性）やRAM40（記憶揮発性）と、NIC10若しくはICU20で処理されたデータをシート材に画像形成を行うことによって出力する画像形成部70の制御を行うプリンタコントローラユニット60（以下、「PCU60」と称する。）と、ユーザがプリンタAに対して操作、入力を行うための操作部50とを具備して構成されている。ここで、上記要否判断機能、上記記憶形式判別機能、上記復元化機能について説明する。

【0013】上記要否判断機能とは、ホスト装置Bより受信したデータに対して暗号化が必要か否かを判断する機能であって、プログラム或いは回路によって実現されるものである。これらのプログラム又は回路が要否判断手段の一例である。上記記憶形式判別機能とは、HDD30、RAM40などの記憶装置が、どのようにしてデータを記憶するのか、或いは、記憶したデータに対して揮発性若しくは不揮発性の特性を有するのか等の記憶形式を判別する機能であって、プログラム或いは回路によって実現されるものである。これらのプログラム又は回路が記憶形式判別手段の一例である。上記復元化機能とは、暗号化された暗号化データをPCU60を介して画像形成部70で印刷出力可能なように上記暗号化データを復元する機能であって、プログラム或いは回路によって実現されるものである。これらのプログラム又は回路が復元化手段の一例である。また、上述において、上記3つの手段はNIC10によって具備されるものとしたが、もちろんNIC10に限定されて具備されるものではなく、独立してプリンタA内部に存在しても良い。

【0014】次に、図2を用いて、暗号化処理装置を採用するプリンタAが行う一連の処理について説明する。

以下の説明では、主にNIC10が判断等の処理を行うものとして説明するが、同様の処理を例えばICU20が行うものとしても良い。処理はステップS10より開始される。NIC10は、ホスト装置BよりプリンタAで印刷出力されるデータを受信する（S10）。ステップS10の処理に続いて、NIC10はプリンタAの記憶装置（HDD30、RAM40）の記憶形式の判別を行う（S20）。このステップS20で行われる処理の詳細を図3を用いて説明する。

【0015】先ず、ステップS20の処理が行われる前提について説明する。このステップS20では記憶装置の記憶形式を判別するのであるが、この場合、上記判別の基準となる記憶装置の型番、記憶形式等の製品データ（揮発性、不揮発性等）が予めNIC10若しくはICU20に記憶されており、該製品データと記憶装置のデバイスドライバの情報とに基いて、NIC10若しくはICU20が上記判別を行うものとする。（以下では上述の通りNIC10が処理するものとする。）先ず、上記製品データとデバイスドライバとに基いて、プリンタAが具備する記憶装置（HDD30、RAM40）のデータ記憶領域の揮発性について判断を行う（S21）。つまり、プリンタAの電源が切断された場合に、記憶装置のデータ記憶領域のデータが揮発するか否かが判断される。この判断で、揮発すると判断された場合はプリンタAが具備する記憶装置のデータの保存性が低いと判別され（S25）、一方、揮発しないと判断された場合は処理がステップS22へ移行する。次に、上記ステップS21と同様に、上記製品データとデバイスドライバとに基いて、プリンタAが具備する記憶装置がプリンタAから取り外された場合に、データ記憶領域のデータが揮発するか否かが判断される（S22）。この判断で、揮発すると判断された場合はプリンタAが具備する記憶装置のデータの保存性が低いと判別され（S25）、一方、揮発しないと判断された場合は処理がステップS23へ移行する。更に、上記ステップS21、22同様に、上記製品データとデバイスドライバとに基いて、プリンタAが具備する記憶装置がプリンタAから取り外された場合に、データ記憶領域のデータが第三者によって読み込み不能な形式のデータに変換するか否かが判断される（S23）。この判断で、変換すると判断された場合はプリンタAが具備する記憶装置のデータの保存性が低いと判別され（S25）、一方、変換しないと判断された場合はデータの保存性が高いと判断される（S24）。このようにして、記憶装置の記憶形式がデータの保存性の高いものであるか否かが判別される。

【0016】上記ステップS20の該判別結果に基いて、NIC10は上記データに対して暗号化が必要か否かの判断を行う（S30）。つまり、上記ステップS30で行われる処理は、上記ステップS20において、記憶装置の記憶形式が保存性の低い形式であると判別され

た場合は、データに対して暗号化が不必要という判断がなされ、一方、上記ステップS20において、記憶装置に記憶形式が保存性の高い形式であると判別された場合は、データに対して暗号化が必要であると判断するものである。そして、データに対して暗号化が不必要と判断された場合は、処理がステップS80へ移行してデータがHDD30又はRAM40に記憶される(S80)。一方、データに対して暗号化が必要と判断された場合は、処理がステップS40へ移行する。

【0017】ここで、図2で示すフローチャートのステップS40以降の説明に先立って、ホスト装置Bで行われる前提となる処理について図7を用いて説明する。ユーザによって、ホスト装置B側で作成されたデータの印刷指示がホスト装置Bに入力される(S210)。つまり、このステップS210の印刷指示の入力時に、ユーザによって「データをホスト装置Bで暗号化するか」、「データをプリンタAで暗号化するか」、「データに親展、重要度等のフラグを付すか」等の暗号化に関する条件の入力が行われる。この条件の入力は、ホスト装置Bが具備する条件付加手段によって行われる。具体的には、上記条件の選択又は指定を行うための表示が、ユーザがデータ入力を行っているホスト装置Bの端末機(不図示)の画面上に、GUI(Graphical User Interface)でアイコンやウィンドウ形式で容易に入力できるように表示されることで、上記条件の入力が行われる。次に、ホスト装置Bは、上記ステップS210におけるユーザの入力に基づいて、データをホスト装置Bで暗号化するか否かの判断をする(S220)。ステップS220の判断で暗号化すると判断された場合は、上記データをホスト装置B側で暗号化し、該暗号化がされたことを示す暗号化フラグを該暗号化されたデータに付す(S230)。そして、ホスト装置Bは上記暗号化されたデータをプリンタAに送信する(S260)。一方、上記ステップS220で、データをホスト装置Bで暗号化しないと判断された場合は、処理がステップS240に移行する。ホスト装置Bは、上記ステップS210でユーザによって入力された印刷指示の中に、上記印刷に関わる条件が入力されているか否かを判断する(S240)。このステップS240で、上記印刷に関わる条件が入力されていると判断された場合に、ホスト装置Bはその旨を示した指標を上記データに対して付す(S250)。そして、ホスト装置Bは上記指標が付されたデータをプリンタAに送信する(S260)。一方、ステップS240で、上記暗号化に関する条件が入力されていないと判断された場合は、データに対してホスト装置B側で何も手を加えずにプリンタAに送信する(S260)。このように、ホスト装置BよりプリンタAに送信されるデータには、プリンタAにおいてデータを暗号化するか否かを判断する際の判断基準となる指標がデータに付加される。つまり、上記指標等に基づ

いて、プリンタAは以下でデータを暗号化するか否かの判断を行う。

【0018】図2のステップS40において、NIC10は、受信したデータの形態が既に暗号化されているのか否かを判断し(S40)、暗号化されていると判断した場合は、上記データをHDD30又はRAM40に記憶する(S80)。一方、上記ステップS40で、上記データが暗号化されていない形態と判断された場合は、処理がステップS50へ移行する。また、上記ステップS40におけるデータが暗号化されているか否かの判断は、例えば、データが上述の暗号化フラグを具備しているか否かを判断することで可能となる。

【0019】ステップS50では、NIC10によって上記データが具備する項目、即ち重要度に関する指標に基づいて、該データの重要度が判別される(S50)。このステップS50で行われる処理の詳細は図4に示ようになる。先ず、上記データに対してデータの保存を指示するような指標の一例であるフラグが付されているか否かを判断する(S51)。上記ステップS51で、上記データに上記フラグが付されていないと判断された場合は、上記データは保存する必要が無い、即ち上記データは揮発しても構わないという程度の重要度しか無いもの(重要度低)と判断される(S55)。一方、上記ステップS51で、上記フラグが付されていると判断された場合は、処理がステップS52に移行して、親展フラグが付されているか否かが判断される(S52)。上記ステップS52で、上記データに上記親展フラグが付されていないと判断された場合は、重要度が低いと判断される(S55)。一方上記親展フラグが上記データに付されている場合は、上記データは重要度が高いと判断される(S54)。このように判断がなされることで、データの保存指示と親展フラグとが共にデータに付されている場合に、該データは重要度が高いと判別される。ここで、再び図2を用いて説明する。

【0020】上記ステップS50におけるデータの重要度(重要度高い(S54)、重要度低い(S55))判別結果に基づいて、NIC10は上記データに対して暗号化が必要か否かの判断を行う(S60)。つまり、上記ステップS60で行われる処理は、上記ステップS50で重要度が低いと判別されたデータに対しては暗号化の必要が無いと判断し、一方上記ステップS50で重要度が高いと判別されたデータに対しては暗号化の必要があると判断するものである。そして、上記データに対して暗号化が不必要と判断された場合は、処理がステップS80へ移行してデータがHDD30又はRAM40に記憶される(S80)。一方、上記データに対して暗号化が必要と判断された場合は、処理がステップS70へ移行して暗号化が施される(S70)。そして、ステップS70で暗号化された暗号化データをHDD30又はRAM40に記憶する(S80)。プリンタAにおいて、

受信したデータを暗号化するか否かの判断の処理が、上述のように行われることで、暗号化が必要と認められるデータのみを暗号化することが可能となり、効率良く上記データを記憶装置に一旦記憶して出力することが可能となる。

【0021】また、上述の処理で暗号化された後に記憶装置（HDD30、RAM40）に記憶されたデータをプリンタAより出力する処理について、図6を用いて以下に説明する。NIC10は、ユーザによって操作部50に出力指示が入力されたか否かを判断する（S90）。そして、上記入力となされた場合に、ステップS70で暗号化されたデータが復元されて印刷出力される（S100）。また、上記ステップS90において、上記出力指示の入力の際にデータのパスワードやIDを入力することによって、該データを印刷出力するようにしても良く、このようにすることで更に該データの安全性が高められる。

【0022】

【実施例】上記実施の形態におけるステップS50の「データの重要度判別」の処理の替わりに、データが予め定められた条件を具備するか否かを判別する処理（S50a）を行っても良い。もちろんこの場合も、ホスト装置Bにおいて、予め定められた条件が図7のステップS210でユーザによって入力されているとする。この判別を行う一連の処理を図5を用いて説明する。NIC10は、データが、予め定められた条件の1つである「ジョブ名称」を具備するか否かの判断を行う（S51a）。ステップS51aで、データが「ジョブ名称」を具備すると判断された場合は、上記データが上記条件を具備するものであると判別する（S54a）。一方、ステップS51aで、データが「ジョブ名称」を具備しないと判断された場合は、処理がステップS52aへ移行する。ここで、上記「ジョブ名称」とは、例えば、会社組織における職制上の役職名のことである。つまり、一般的に、役職をもった人ほど仕事上の責任が増加すると共に扱う文書やそのデータの機密性も高まるといえるので、データが上記「ジョブ名称」を具備するものか否かを判別した結果が、図2のステップS60において、データに対して暗号化が必要か否かの判断を行う際の判断基準となる。

【0023】続いて、ステップS52aでは、データが、予め定められた条件の1つである「暗号化の指示」を具備するか否かの判断がなされる（S52a）。この「暗号化の指示」とは、例えば、データの内容が機密事項を含むものであることを示すフラグのようなものであり、該フラグが上記データに具備されているか否かを上記ステップS52aで判別した結果が、上述同様に図2のステップS60において、データに対して暗号化が必要か否かの判断を行う際の判断基準となる。上記ステップS52aで、上記データが上記「暗号化の指示」を具

備しないと判断された場合は、上記データが上記条件を具備しないものと判別される（S55a）。一方、上記データが上記「暗号化の指示」を具備すると判断された場合は、上記条件を具備しないものと判別される（S54a）続いて、図2のステップS60の処理が行われ、上記データが上記条件を具備しない場合は、上記データに対して暗号化が不必要と判断され、一方上記データが上記条件を具備する場合は、上記データに対して暗号化が必要と判断される（S60）。以降の処理は上記実施の形態と同様の処理が実行される。このように、ステップS50「データの重要度判別」に替えて、ステップS50aとしてデータが予め定められた条件を具備するか否かを判別する処理を実行うすることで、ステップS60で行う判断の判断基準を定めることが可能となる。

【0024】

【発明の効果】本発明は、受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置において、上記データに対して暗号化が必要か否かを判断するための要否判断手段を具備し、上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化することを特徴とする暗号化処理装置として構成されている。本発明がこのような構成されているので、受信したデータの中で暗号化が必要と認められるデータのみを暗号化することによって、従来に比べて効率良く記憶装置に上記データを記憶して出力することが可能となる。また、暗号化が不要なデータについては暗号化されないで、処理の迅速性が維持される。

【0025】本発明において、前記要否判断手段は、前記記憶装置の記憶形式を判別するための記憶形式判別手段の判別結果に基づいて、上記データに対して暗号化が必要か否かを判断するように構成されても良い。このように構成されることで、第3者によって前記記憶装置が盗難にあった場合のデータの読み出しの可能性が判別できるので、例えば、前記記憶装置のデータの保存性が低ければ盗難時にデータが消滅するので、データに対して暗号化する必要が無くなり、更に不要な暗号化を防止できる。また、前記記憶形式判別手段によって、前記記憶装置は単体で存在する状況においても記憶している前記データを前記受信の際の状態で保存すると判別された場合に、更に前記要否判断手段は前記データに対して暗号化が必要と判断しても良い。この場合も、上述同様に、前記記憶装置単体が盗難に遭ったとしても前記データの内容が第3者によって解読される可能性が無く、前記データが機密性の高いデータである場合に非常に有効である。

【0026】また、前記要否判断手段は、前記データの形態又は具備する項目に基づいて、前記データに対して暗号化が必要か否かを判断するよう構成されることが望ましい。このように前記要否判断手段が判断することによって、暗号化が必要と認められる受信データのみを選択

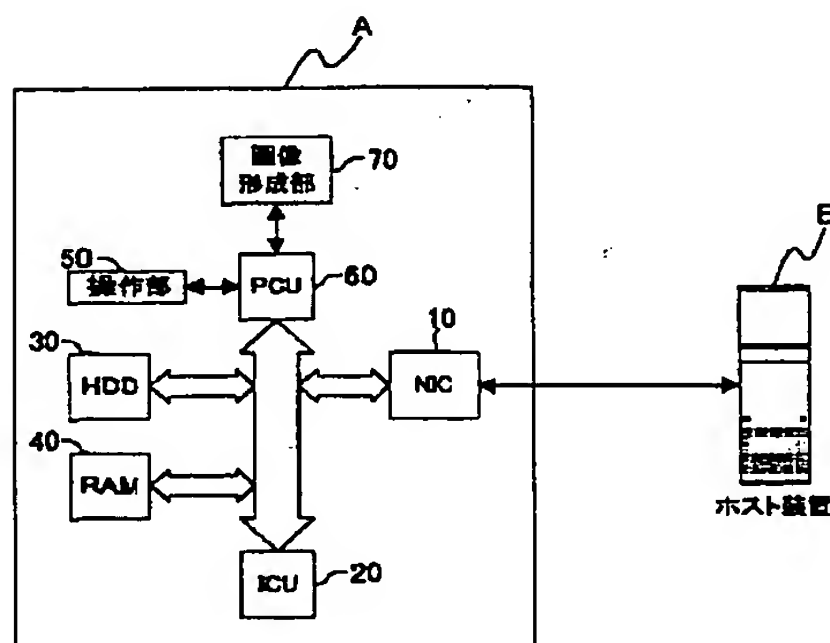
的に暗号化することが可能となり、従来の技術に比べて効率的に前記データの暗号化を実施することが可能となる。更に、前記データの形態が既に暗号化されている場合に、前記要否判断手段は前記データに対して暗号化が不必要と判断、又は、前記データの具備する項目が前記データの重要度に関する指標（フラグ、親展指示）である場合に、前記要否判断手段は前記データに対して暗号化が必要と判断、又は、前記データの具備する項目が予め定められた条件である場合に、前記要否判断手段は前記データに対して暗号化が必要と判断するように構成しても良い。このように構成することで、上述同様に、前記要否判断手段によって、暗号化が必要と認められる受信データのみを効率良く選択的に暗号化することが可能となる。

【0027】前記記憶装置に暗号化して記憶されている前記データを復元するための復元化手段を具備し、該復元化手段によって前記データが復元された後に前記データが出力されるように構成することが望ましい。このように本発明に復元化手段が設けられることによって、暗号化が必要と認められて暗号化された前記データを自動的に復元化して出力することが可能となる。

【0028】また、上述の暗号化処理装置の用途として前記データの受信側の機器に採用されても良く、例えば、本発明の暗号化処理装置をホスト装置とプリンタとで構成される印刷システムに採用することで、暗号化を施すべき文書のみを効率良く印刷出力することが可能となる。

【0029】また本発明をシステムとして捉えると、データの作成などのサービスを提供するホスト装置と、該ホスト装置より受信したデータを暗号化して記憶装置に記憶した後に、該データを出力する暗号化処理装置とを具備した暗号化処理システムにおいて、上記ホスト装置は、データを上記暗号化処理装置に送信する際に、該データに対して暗号化に関する条件を付加する条件付加手段を具備し、上記暗号化処理装置は、上記条件の有無に基づいて、上記データに対して暗号化が必要か否かを判断*

【図1】



* するための要否判断手段を具備し、上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化処理装置側で暗号化することを特徴とする暗号化処理システムとして構成されている。本発明がこのような構成されているので、暗号化処理装置の要否判断手段は、上記ホスト装置側で付加された暗号化に関する条件がデータに付加されているか否かを容易に判断できるので、受信したデータの中で暗号化が必要と認められるデータのみを暗号化することが可能となる。

10 【図面の簡単な説明】

【図1】本発明の実施の形態に係る暗号化処理装置を採用するプリンタAの概略構成図。

【図2】本発明の実施の形態に係る暗号化処理装置を採用するプリンタAが行う一連の処理手順を示すフローチャート。

【図3】図2のステップS20のサブルーチンの一連の処理を示すフローチャート。

【図4】図2のステップS50のサブルーチンの一連の処理を示すフローチャート。

20 【図5】図2のステップS50のサブルーチンの別例の一連の処理を示すフローチャート。

【図6】プリンタAが行う復元処理を示すフローチャート。

【図7】ホスト装置Bが行う条件付加の処理を示すフローチャート。

【符号の説明】

A……………プリンタ（暗号化処理装置採用）

B……………ホスト装置

10……………NIC

30……………HDD（不揮発性）

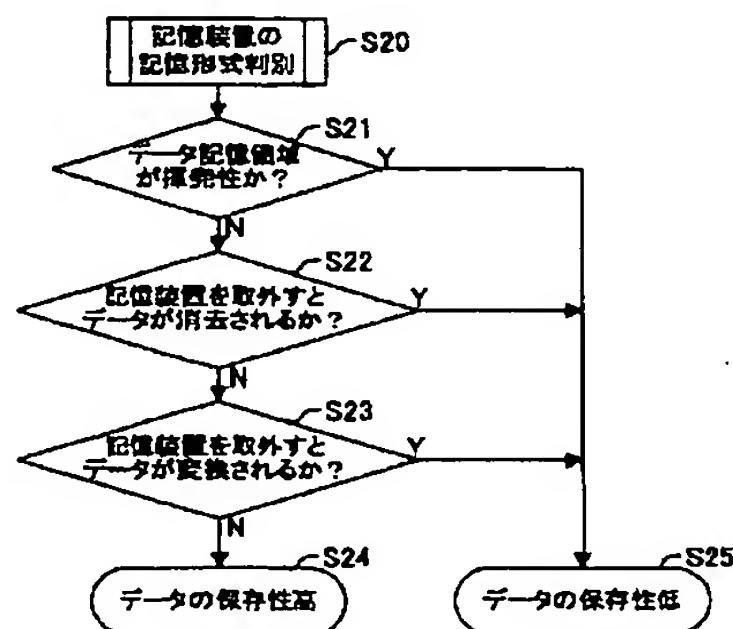
40……………RAM（揮発性）

50……………操作部

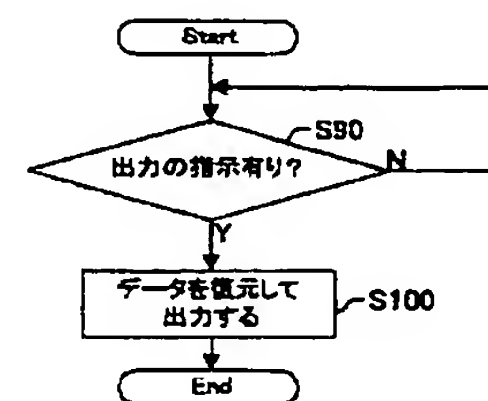
60……………PCU

70……………画像形成部

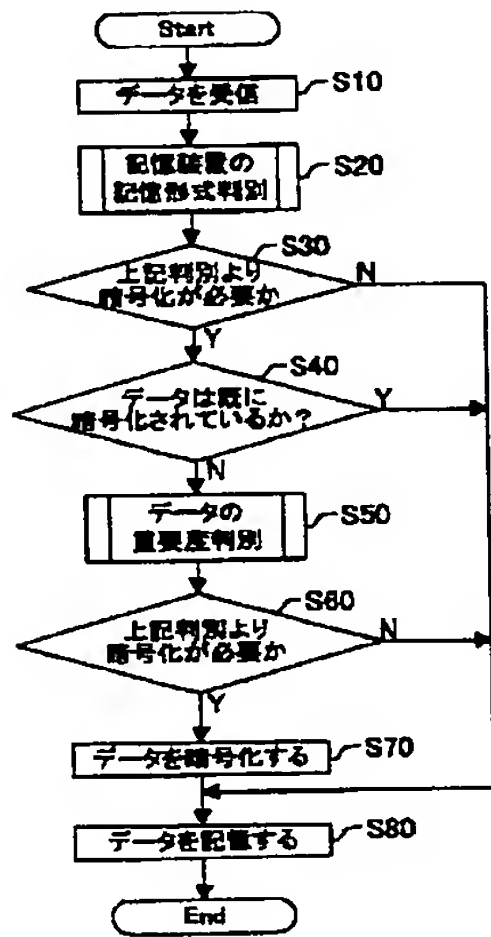
【図3】



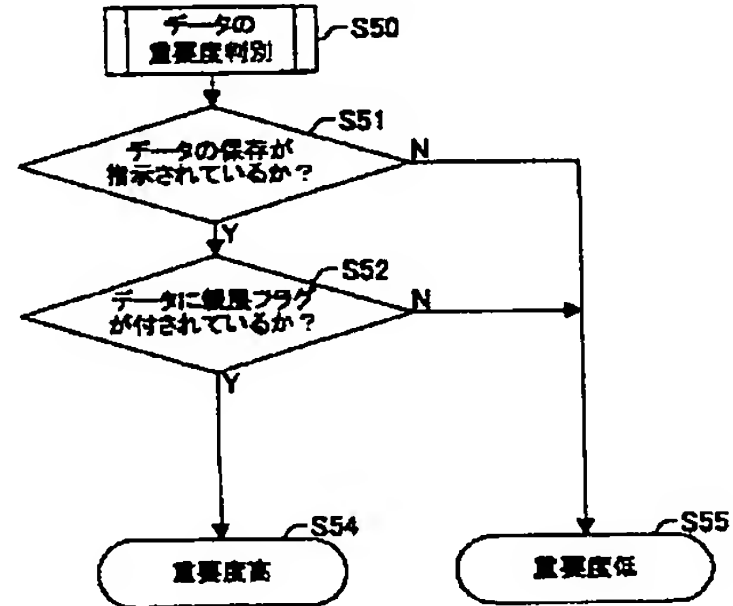
【図6】



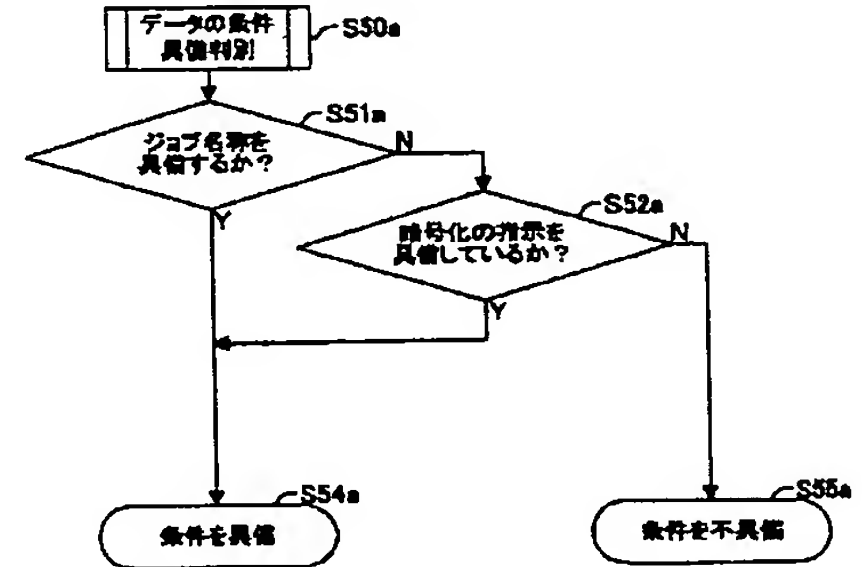
【図2】



【図4】



【図5】



【図7】

